MISSOURI DEPARTMENT OF MENTAL HEALTH

KEITH SCHAFER, DEPARTMENT DIRECTOR

DEPARTMENT OPERATING REGULATION NUMBER
DOR 8.370

CHAPTER	SUBCHAPTER	EFFECTIVE DATE	NUMBER OF PAGES	PAGE NUMBER
Regulatory Compliance	HIPAA Regulation	April 9, 2014	3	1 of 3

SUBJECT	AUTHORITY	
Security Maintenance	630.050	History: See below

PERSON RESPONSIBLE	SUNSET DATE
General Counsel	Julv 1. 2017

Purpose: The Missouri Department of Mental Health (DMH) is committed to maintaining formal practices to monitor the receipt and removal of hardware and electronic media that may contain electronic protected health information into and out of its facilities. In addition, DMH will prescribe practices to ensure continuity of operations. DMH shall continue to develop, implement and maintain appropriate administrative, physical and technical security measures in accordance with 45 CFR 164.310(d).

Application: DMH, its facilities and workforce.

(1) Definitions

(A) DMH Workforce – Includes all state employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity (facility or Department). This shall include client workers employed by the Department of Mental Health or its facilities.

(B) Chief Security Officer (CSO) – Individual designated to oversee all activities related to the development, implementation, maintenance of, and adherence to DMH and facility policies and procedures covering the electronic and physical security of, and access to, protected health information and other DMH data in compliance with federal and state laws and regulations.

(C) Electronic Protected Health Information (EPHI) — individually identifiable health information that is transmitted or maintained in electronic media, or transmitted or maintained in any other form or medium.

(D) ITSD – Information Technology Services Division of the Missouri Office of Administration.

(2) General

(A) The policies and procedures stated herein apply to all EPHI maintained or transmitted by or for DMH.

(B) Receipt, removal, backup, storage, reuse and disposal of EPHI into or out of a facility, as well as throughout the facilities operated by DMH shall be governed by the policies and procedures herein.

(C) The policies and procedures herein also apply to the hardware on which data is stored.

(3) Procedures

(A) Procedures for hardware tracking:

1. ITSD will inventory and track computer hardware used for DMH systems and users using ITSD's electronic tracking system. This shall include movement and disposal of hardware.

2. ITSD shall use automation to install standard software to include malware protection on all hardware to be used by DMH workforce or for DMH electronic systems. This does not preclude using non-automation for non-standard software or individual use packages.

3. All mobile devices including laptops, portable medical carts, and tablets shall be encrypted using the state standard encryption software.

(B) Backup and storage of hardware and/or software containing EPHI:

1. DMH data shall be backed up nightly.

2. Backups shall be kept for a minimum of thirty (30) days but longer for critical data or to meet state and/or federal regulations. These retention schedules shall be established by DMH and communicated to ITSD.

3. Backups shall be kept at a location other than where the data resides but be readily available in the event data needs to be restored.

4. Backups shall be tested a minimum of monthly to ensure a good backup was performed and data can be restored.

5. These duties shall be performed by designated ITSD staff.

(C) Disposal of electronic data, hardware and/or software:

1. ITSD shall ensure protected health information has been destroyed. All computer systems, electronic devices and electronic media must be properly cleaned of sensitive data and software before being transferred outside of DMH either as surplus property or as trash. Computer hard drives must be cleansed by using disk wiping software that is compliant with Department of Defense standards. Non-rewritable media, such as CDs or non-usable hard drives, must be physically destroyed. Hard drives may not be returned to a vendor for credit even if determined inoperable.

2. Other devices that store data, such as copiers, printers, and medical devices, must be cleansed of any data before leaving a DMH facility.

(D) Reuse of media and devices that contain EPHI, including hardware and/or software:

1. ITSD shall use imaging software to install an image to overwrite any data previously on the hardware to ensure past data cannot be retrieved.

2. ITSD shall ensure disks have been properly cleaned from servers that may include EPHI.

(E) Information Security Procedures:

1. Access to DMH networks from public networks shall be protected by access control systems such as firewalls, access control lists, and user authentication under the auspices of designated ITSD staff.

2. Malware protection for all devices used by DMH workforce and systems shall be maintained by designated ITSD staff, pursuant to the virus protection guidelines below.

a. All servers used by DMH systems shall be protected using the State standard anti-malware product.

b. All workstations, laptops, tablets and other devices that connect to the consolidated state network shall be protected using the anti-malware software for that device

as prescribed by the State standard. The software shall be installed, configured and maintained by designated ITSD staff.

c. Anti-malware server and client software shall be configured by designated ITSD staff to check for signature updates daily.

d. Anti-malware client software shall be configured to conduct a thorough, scheduled scan at least weekly.

e. Anti-malware client software shall be configured to check for new signature updates hourly from the master console of the anti-malware program.

f. Out-of-band virus signature updates created in the event of a known virus shall be manually pushed by designated ITSD staff to all devices within twenty-four (24) hours of the time the receipt of the update has been received at the master console.

g. In the event of a virus outbreak, the Incident Response Procedures maintained by ITSD shall be followed.

3. Software updates, patches and service packs for all devices used by DMH users and systems shall be maintained by designated ITSD staff, pursuant to the procedures listed below.

a. Updates shall be installed monthly after being released on all devices. Periodic audits shall be conducted to ensure devices are in compliance.

b. ITSD shall maintain a support contract with the anti-malware software vendor(s) to ensure uninterrupted support.

4. DMH applications shall be developed to restrict data being cached on user workstations when the application is closed.

(4) A current disaster recovery plan for all of DMH's electronic systems shall be created, tested and maintained by ITSD in conjunction with DMH. The plan shall be approved by DMH.

(5) DOR Control - There shall be no facility policies pertaining to this topic. The Department Operating Regulations shall control.

(6) Sanctions. Failure of workforce members to comply or ensure compliance with the DOR may result in disciplinary action, up to and including dismissal.

(7) Review Process. The Chief Security Officer may assign regular checks to see that all hardware and software receipt is done in accordance with these policies and procedures, and take corrective action as necessary.

History: Original rule effective October 15, 2004. On July 1, 2008 the sunset date was extended to July 1, 2011. Amendment effective July 1, 2008. Amendment effective June 23, 2011. On June 23, 2011 the sunset date was extended to July 1, 2014. Amendment effective April 9, 2014.